PROCEEDINGS

OF THE

NATIONAL ACADEMY OF SCIENCES

Volume 1 JANUARY 15, 1915 Number 1

RECENT PROGRESS IN THE THEORIES OF MODULAR AND FORMAL INVARIANTS AND IN MODULAR GEOMETRY

By L. E. Dickson

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO

Presented to the Academy, November 7, 1914

1. Contrast between algebraic and modular invariants. By way of introduction we recall the argument, made in certain texts on invariants, to prove that a linear form $l = ax + by$ has no invariant. For, the vanishing of an invariant $I\ (a, b)$ of l would imply a property of those forms l for which $I = 0$, not possessed by the forms l for which $I \neq 0$. But all forms l are equivalent since each can be transformed into x. This argument is erroneous since the identically vanishing form l (with $a = b = 0$) cannot be transformed into x. Nor is the conclusion correct. The function $I\ (a, b)$, defined in the sense of Dirichlet to be unity if $l \equiv 0$ and zero if l is not identically zero, is evidently an invariant of l, since it has the same value for all equivalent forms l.

In the number-theoretic case in which the coefficients of l and of the linear transformation are integers taken modulo p (a prime), the bizarre Dirichlet function $I\ (a, b)$ employed in the algebraic case is no longer necessary, since it may now be replaced by the polynomial invariant

$$I = (a^{p-1} - 1)(b^{p-1} - 1),$$

with the value unity if $a \equiv b \equiv 0 \pmod p$ and the value zero if a and b are not both congruent to zero. Hence I is an invariant of l modulo p. It is called a *modular* invariant of l.

2. Formal invariants and their construction. Let the coefficients a and b of l be independent variables as in the theory of algebraic invariants. But let the coefficients of the linear transformations be integers taken modulo p as in the theory of modular invariants. Invariants arising in this composite case are called formal invariants and were first introduced by Hurwitz.[1] Although a remarkably simple theory of modular invariants has been given,[2] no headway was made towards a theory of formal invariants before the very recent discovery[3] of a simple effective method for their construction. This method will be illustrated for the linear form l and the modulus 2. The real points (i.e., those with integral coördinates) modulo 2 are $(1, 0)$, $(0, 1)$ and $(1, 1)$. The values of l at these points are a, b, $a + b$. Any real linear transformation induces a permutation of these three values since it merely permutes the three real points. Hence any symmetric function of these three values is a formal invariant of l. The elementary symmetric functions reduce modulo 2 to zero, $i = a^2 + ab + b^2$ and $j = ab\,(a + b)$. We pass to modular invariants by taking a and b to be integers modulo 2. Then $j \equiv 0, i \equiv I + 1$, where I is the invariant in § 1.

In treating similarly the formal invariants of l modulo 5, we would employ the symmetric functions of the fourth powers of our values a, b, $a + b$, and not the values themselves. For, $(1, 0)$, $(2, 0)$, $(3, 0)$, $(4, 0)$ give the same point and yet lead to the values a, $2a$, $3a$, $4a$ of l; we take the fourth power to secure a value uniquely defined by the point. In the case of a quadratic form modulo 5, we need only take the squares of the values.

The method is applicable to invariants of several forms in any number of variables and to semi-invariants, as shown in the paper cited, which gives also a novel method of deriving modular invariants from semi-invariants.

3. Modular plane curves for modulus 2. Let $f\,(x, y, z)$ be a homogeneous form of degree n with integral coefficients. A point for which the three first partial derivatives of f are zero modulo 2 shall be called a *derived point.* If n is even, it need not be a singular point of the curve, since it need not lie on the curve; the argument in the algebraic case, based on Euler's theorem

$$x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z} = nf,$$

does not apply modulo 2 when n is even, since the vanishing of the left member does not require that of f. A non-singular derived point shall be called an *apex* of the curve; its linear polar is indeterminate.

For example, any non-degenerate conic (i.e., having no linear factor modulo 2) can be transformed linearly into $x^2 + yz = 0$. The only derived point is $p = (1, 0, 0)$ and is an apex. Any line through p is tangent to the conic; this is evident for $z = 0$ and follows for $y = kz$ since the elimination of y leads to $x^2 + kz^2 = 0$, with a double root modulo 2. For the theory[4] of quadratic loci modulo 2 in space of any number of dimensions, see the *Madison Colloquium Lectures*, p. 65.

The next case, $n = 4$, for which apices occur presents other remarkable peculiarities.[5] Whereas in the algebraic case a quartic curve has 28 bitangents in general, one in the case of modulus 2 has at most 7 bitangents and usually exactly 7. The bitangents intersect at derived points and usually all of the derived points are intersections of bitangents. An interesting example is given by

$$K = x^4 + y^4 + z^4 + x^2y^2 + x^2z^2 + y^2z^2 + xyz\,(x + y + z),$$

an invariant under all real linear transformations. Here real is used in the sense of integral; likewise for the real points $(1, 0, 0), \ldots, (1, 1, 1)$ modulo 2. The bitangents to $K = 0$ are the 7 real lines in the plane and their interesections are the 7 real points, the latter being apices and not singular points.

A quartic curve containing all seven real points and having no linear factor modulo 2 can be transformed into

$$x^3y + x^2y^2 + xz^3 + x^2z^2 + y^3z + yz^3 = 0.$$

It has no singular point and has the 7 apices $(1, z^3, z)$, where $z^7 + z^3 + 1 = 0$. Its 7 bitangents are $x = (b^3 + 1)\,y + bz$, where $b^7 + b + 1 = 0$; they intersect at apices. Each apex is on three bitangents, while three apices are on each bitangent. The configuration of the apices and bitangents, here all imaginary, is entirely similar to that for K, composed of real elements.

The classification of quartic curves is similar to that next illustrated for the simpler case of cubic[6] curves modulo 2.

A cubic curve containing all seven real points is of the form

$$a\,(x^2y + xy^2) + b\,(x^2z + xz^2) + c\,(y^2z + yz^2) = 0.$$

If not zero identically, it can be transformed into $x^2y + xy^2 = 0$. A cubic curve containing just two real points can be transformed into one containing $(1, 0, 0)$ and $(0, 1, 0)$; the transformations leaving the latter fixed or permuting them are available for the specialization of the parameters in the coefficients of the cubic. In this way we find the 21 types of non-equivalent cubics, including degenerate curves, and see that they are completely characterized by the number of real points, real inflexion points, real and imaginary singular points,—geometrical invariants easily expressed by modular invariants.

For the determination of the inflexion points of the cubic $n\,(x_1, x_2, x_3) = 0$ modulo 2, the Hessian of n is not available, being identically zero modulo 2. In its place we may employ the function

$$C = \xi_1\xi_2\xi_3 + \Sigma\,\xi_i\eta_i^2 + k\Sigma x_1\xi_1\eta_1 + k\Sigma x_1\eta_2\eta_3 + k^2\Sigma x_1x_2\eta_3 + k^3x_1x_2x_3,$$

in which $n = v + kx_1x_2x_3$, while the quotients

$$\xi_i = \tfrac{1}{2}\frac{\partial^2 v}{\partial x_i^2},\ \eta_1 = \tfrac{1}{2}\frac{\partial^2 v}{\partial x_2\,\partial x_3},\ \cdot\cdot\cdot,\ \eta_3 = \tfrac{1}{2}\frac{\partial^2 v}{\partial x_1\,\partial x_2}$$

have integral coefficients. The points of inflexion of $n = 0$ are its intersections with $C = 0$. Although C is not a covariant, it forms with n a covariant pencil, since C is transformed into a linear function of n and C.

[1] Hurwitz, *Arch. Math., Leipzig*, ser. 3, 5, 25, (1903).

[2] Dickson, *Madison Colloquium Lectures*, American Mathematical Society, (1914).

[3] Dickson, *Trans. Amer. Math. Soc.*, 15, 497, (1914).

[4] An advance in the theory of seminvariant leaders of covariants of quadratic forms has been made recently by the writer, *Bull. Amer. Math. Soc.*, January, 1915.

[5] Dickson, *Trans. Amer. Math. Soc.*, April, 1915.

[6] MS. offered Aug. 4, 1914 to *Amer. J. Math.* To appear April, 1915.

THE SYNTHESIS OF TRIAD SYSTEMS Δ_t in t ELEMENTS, IN PARTICULAR FOR t = 31

By Henry S. White

DEPARTMENT OF MATHEMATICS, VASSAR COLLEGE

Presented to the Academy, December 3, 1914

Purely theoretical interest first led to the study of triad systems Δ_t in t elements; systems of threes or triads, that is, in which every possible pair of elements is found in some one triad, but only one. Their relation to other objects of research in algebra and geometry began to appear when Noether (1879) pointed out the peculiar nature of a resolvent equation of the seventh degree which had been found by Betti, Hermite, and Kronecker in discussing the transformation of the seventh order of elliptic functions. This modular equation has roots related in triads like the Δ_t. Hesse had shown earlier, in plane curves of the third order, that the nine inflexion points lie by threes on twelve lines, thus exemplifying a Δ_9. Noether succeeded also in connecting the Δ_7 with the important sets of double tangents to the plane quartic curve which Aronhold had introduced under the name of *Siebenersysteme*. With those important applications in hand, and ten or twelve known Δ_{15}'s to serve as further data, mathematicians took up with renewed interest the question whether there are actual triad systems for every suitable member t of elements, i.e., for t = 13, 15, 19, 21, 25, 27, etc.; or precisely, t = 6k + 1 or 6k + 3.